

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In re Search Warrant No. 16-960-M-1 : Misc. No. 16-960-M-01
to Google :
: FILED UNDER SEAL

GOOGLE INC.'S RESPONSE TO OCTOBER 23, 2016 ORDER TO SHOW CAUSE AND
MOTION TO AMEND NON-DISCLOSURE ORDER

I. INTRODUCTION

The government seeks to compel Google to produce electronic records relating to three user accounts—records that Google either does not have or cannot lawfully disclose under *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. (Microsoft)*, 829 F.3d 197 (2d Cir. 2016) (“*Microsoft*”). The government seeks to obtain these records under the auspices of an overbroad search warrant that fails to identify with particularity which Google services it has established probable cause to search. Google has already provided all records in its possession that the government may lawfully compel Google to produce. The government’s motion should therefore be denied.

The government also obtained a non-disclosure order that imposes an indefinite prior restraint of Google’s free speech, prohibiting Google from notifying the customers whose accounts are to be searched. The Stored Communications Act requires that the court designate a period during which a provider may be prohibited from notifying its customer, and the First Amendment requires that any such prior restraint remain in effect only as long as necessary to accomplish a compelling government interest.

II. FACTUAL BACKGROUND

On August 5, 2016, Google received a search warrant (dated August 2, 2016) purporting to compel Google to disclose all electronic records relating to three Google accounts from

November 10, 2008, through January 1, 2016. *See* Search and Seizure Warrant, Attachs. A (“Property to be Searched”), B (“Particular Things to be Seized”).¹ The warrant did not limit its scope to records stored in the United States or particularly identify specific Google services the government had probable cause to believe might contain evidence of a crime. *Id.* It broadly authorized the government to obtain records that were from or related to “all Google Services” ever used by the subject accounts, devices used to access those accounts, and “communications between Google and any person regarding the Account[s].” *See id.* The warrant was accompanied by a nondisclosure order (“NDO”) prohibiting Google indefinitely from disclosing the existence of the search warrant or NDO to any person aside from an attorney for purposes of obtaining legal advice. *See* Order (Aug. 2, 2016).

On August 18, 2016, Google produced all reasonably available records for the subject accounts that it could determine were stored in the United States for services implicitly specified in the Warrant. Declaration of John R. Tyler in Support of Google’s Opposition (“Tyler Decl.”) ¶ 2, Ex. A. This included basic subscriber information, contacts, search history, browsing history, Android, and all Gmail content it was able to determine were stored in the United States from each of the three subject accounts, as well as location data for one account. *Id.* Consistent with *Microsoft*, the production did not include any emails with attachments because, given the nature of Google’s distributed systems, such attachments were not confirmed to be stored in the United States. The production was accompanied by a letter specifying that Google produced

¹ Specifically, the warrant purports to authorize the government to obtain from Google “[t]he contents of all communications and related transactional records” and “all data and related transactional records” for “all Google Services ever used by” the subject accounts; “[a]ll records and information concerning any Android device ever associated with the” subject accounts; “[a]ll records of web search and browsing history,” “[a]ll device or user identifiers linked to the Account[s] at any time”; “[a]ll records or other information regarding identification of the Account[s]”; and “[a]ll records of communications between Google and any person regarding the Account[s], including contacts with support services and records of actions taken.” *See id.*

responsive records in a manner consistent with the SCA and the Second Circuit's decision in *Microsoft*.

On October 28, 2016, the government filed a motion to compel Google to produce additional information, with Google's response due November 14, 2016.

On November 10, 2016, based on newly developed tooling, Google informed the government that it would produce additional responsive information. Tyler Decl. ¶ 3, Ex. B.

On November 11, 2016, Google and the government agreed via email to stipulate to continue Google's response deadline in order to provide the government time to review Google's supplemental production. Tyler Decl. ¶ 3, Ex. B. That same day, Google provided a supplemental production containing additional header information associated with the emails that had attachments, as well as the content of those email messages (but not the attachments, which were not confirmed to be stored in the United States). *Id.* ¶ 4, Ex. C. To date, the government has obtained all responsive records related to the targeted Gmail accounts that Google is able to produce consistent with the current state of the SCA. *Id.* ¶ 5.

III. ARGUMENT

Google has already produced in good faith the electronic records that are responsive to the warrant and that Google knows to be maintained within the geographic reach of the warrant. The government has nonetheless moved to compel Google to produce additional records.

Google cannot, consistent with applicable laws, produce additional records for three reasons. First, under the Second Circuit decision in *Microsoft*, a warrant issued by a U.S. court pursuant to the Stored Communications Act ("SCA") can only compel the production by a provider of electronic records stored within the United States. Second, Google cannot produce records that it does not have, and as the government is now aware, Google has not withheld any existing emails dated before October 13, 2013. Third, the warrant is overbroad, vague, and

lacking sufficient particularity insofar as it requests all records from all Google services ever used (of which there are dozens) without particularly identifying which services Google must search, which suggests that the government may not know whether the users in fact used any other services, let alone used them in a manner that may give rise to probable cause to believe that records regarding their use would contain evidence of the alleged wire fraud. The government also served Google with the NDO purporting indefinitely to prohibit Google from disclosing the existence of the warrant or the NDO except to legal counsel. This indefinite nondisclosure order constitutes an unconstitutional prior restraint that violates Google's First Amendment rights.

A. Google Has Fully Complied with the Warrant

1. The Warrant Reaches Only Data Known to be Stored Within the United States

Google has already produced all records identified with sufficient particularity that are responsive to the warrant. A warrant issued under the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.*, lawfully reaches only data stored within the United States. *See Microsoft*, 829 F.3d at 222 ("[T]he SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States."). Google has already produced all records that it can ascertain are stored within the United States. The warrant cannot compel Google to produce records that are or may be stored outside the United States.

In *Microsoft*, a panel of the Second Circuit unanimously held that executing a warrant to obtain data stored outside of the United States "would constitute an unlawful extraterritorial application of the Act." 829 F.3d at 220. The court held that SCA did not authorize the government to compel a U.S. provider to produce electronic records stored in data centers

outside the United States. *See id.* at 210-21. The court observed that the SCA’s “focus” was primarily on protecting user privacy in stored electronic communications, not on law enforcement needs. *See id.* at 221. As a result, the seizure of user information stored outside the United States—regardless of the location of the user or of the service provider—occurs outside the United States and thus constitutes an unlawful extraterritorial application of the SCA. *See id.* at 220. Indeed, the *Microsoft* panel so held even though Microsoft acknowledged it could use a “database management program” from within the United States to collect and produce “account data that is stored on any of its servers globally.” Likewise, the present warrant therefore cannot compel Google to search, seize and produce data in the subject accounts stored outside the United States.

The warrant also cannot reach records where it is unknown whether the records are located in the United States. *See, e.g., In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, 757-58 (S.D. Tex. 2013) (holding that a warrant cannot reach records the location for which is unknown). Indeed, this court has recognized that for traditional search warrants issued pursuant to Fed. R. Crim. P. Rule 41, a magistrate judge lacks authority to issue a search warrant for out-of-district property, even where the location of the property was unknown at the time of issuance. *United States v. Werdene*, ___ F. Supp. 3d ___, 2016 WL3002376 at *7 (E.D. Pa. May 18, 2016) (holding that a Virginia judge lacked authority to issue a warrant to search property the location of which was unknown at the time of issuance, and which was ultimately located in Pennsylvania); *see also* Fed. R. Crim. P. 41(b) (defining territorial limits of search warrants to reach property within the district of the magistrate or, in

certain cases not relevant here, the United States).² By producing the records known to be stored in the US, Google has fully complied with the warrant.

Although as a Second Circuit decision *Microsoft* does not bind this Court, *see* Mot. to Compel at 6, the decision carries heavy persuasive weight, particularly because the government cites no authority to support a contrary position. *See Odoms v. YWCA of Bucks Cty.*, No. CIV.A. 12-7146, 2013 WL 3213355, at *2 (E.D. Pa. June 25, 2013) (noting that although certain Second and Seventh Circuit cases were non-binding, they were “persuasive and provide[d] guidance in resolving the present matter,” whereas the opposing party “present[ed] no precedent” to support its position).³ The warrant therefore compels Google only to produce data known to be stored within the United States. *See Microsoft*, 829 F.3d at 222; 18 U.S.C. §§ 2701, 2703. Google has already produced all records that it can ascertain are stored in the United States.

2. Google Does Not Have, and Therefore Cannot Produce, the “Missing” Emails

Based on subsequent communications with the government, Google understands that the government no longer seeks to compel Google to produce email content from one of the subject accounts dating from before October 13, 2013. *See* Tyler Decl, ¶ 5; Mot. to Compel at 5 & nn.1-2. To the extent the government nevertheless seeks to compel disclosure of this information, there is nothing to produce. As Google has explained, this information simply is not present in its systems. *See Rega v. Beard*, No. CIV.A 08-156, 2010 WL 1253531, at *4

² While Rule 41 will be modified on December 1, 2016, to permit magistrate judges to issue warrants to search out-of-district electronic information in certain circumstances not relevant here, nothing in the amended Rule 41 contemplates a search of property that is or may be located outside the country. Regardless, at the time of the Warrant’s issuance, Rule 41 was plainly insufficient to justify issuance of the warrant to search property where it is unknown if such property is located within the Court’s jurisdiction. *Cf. Werdene*, 2016 WL 3002376 at *7.

³ This would not be the first time the well-reasoned opinion of a single Circuit Court changed as a practical matter the way courts and parties viewed the SCA. *See, e.g., United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding the Fourth Amendment requires the government to obtain a warrant for communications content, notwithstanding section 2703 of the SCA).

(W.D. Pa. Mar. 24, 2010) (denying a portion of a motion to compel because “[d]efendants cannot be made to produce a document that does not exist”).

B. The Warrant Is Overbroad Because It Does Not Describe With Particularity Which Services There is Probable Cause to Search

The warrant is also overbroad to the extent it purports to authorize the government to search the electronic records for *dozens* of different Google services that may (or may not) have been used by the subject accounts without identifying with particularity each service for which the government has established probable cause. *See U.S. v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents* (\$92,422.57), 307 F.3d 137, 149 (3rd Cir. 2002) (“An overly broad warrant describes in both specific and inclusive generic terms what is to be seized, but it authorizes the seizure of items as to which there is no probable cause.”) (internal quotation and citation omitted). Google is concerned that the warrant was not “sufficiently definite and clear so that the magistrate . . . c[ould] objectively ascertain its scope.” *Doe v. Groody*, 361 F.3d 232, 239 (3rd Cir. 2004); *see also U.S. v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982) (a magistrate must be “fully apprised of the scope of the search” and must have “[made] the determination that the search in all of its dimensions is based upon probable cause and particular descriptions”). Although Google is not privy to the affidavit submitted in support of the search warrant application, it seems unlikely that a single affidavit could support a finding of probable cause as to *all* Google services. Asserting that because an account-holder uses Gmail they may use other Google services, too, is not sufficient to establish probable cause as to those other services.

A court determines whether a warrant is overbroad by “compar[ing] the scope of the search and seizure authorized by the warrant with the ambit of probable cause established by the supporting affidavit.” *In re Impounded Case (Law Firm)*, 840 F.2d 196, 200 (3d Cir. 1988).

“Each part of the search authorized by the warrant is examined separately to determine whether it is impermissibly general or unsupported by probable cause.” *United States v. Christine*, 687 F.2d 749, 754 (3d Cir. 1982).

Applying these principles to the SCA warrant at issue here requires the government to establish probable cause to search *each* Google service for which it requests electronic records. *See United States v. Barthelman*, No. 13-10016, 2013 WL 3946084, at *11 (D. Kan. July 31, 2013) (warrants directed to Yahoo! and Apple were overbroad “because they allow[ed] the search of all emails, pictures, friends and groups,” even when they “were limited to a specific account” and “a specific time frame”). Establishing probable cause “that evidence of a crime would be found in the contents of email accounts” is not sufficient to search all the other possible services. *See id.*

It is difficult to believe the government could, in a single affidavit, meet its burden to establish probable cause to believe that each of the three accounts used all of Google’s services during the same time period in such a manner that records associated with those services are likely to contain evidence of wire fraud. Google offers many different services with disparate functionalities, each with its own set of records that may have nothing to do with the records stored by other services. Tyler Decl., Ex. D. For example, Gmail is an email service, so Gmail records would relate to that user’s use of email; Google Maps is a navigational tool and thus the records would relate to a user’s use of a navigational service; Google Analytics is a service offered to users who use Google to host a website, and provides information about the visitors to that website along with detailed reports about the number and type of visits to a page; and Google AdWords is an advertising service and records would relate to advertising campaigns.

Common sense dictates that the facts necessary to support probable cause with respect to an email account would differ from those necessary to support probable cause to search web analytics or advertising records. That an individual has a Gmail account does not give the government carte blanche to scour all Google services for other data the individual may have stored with Google, absent probable cause that such data exists and constitutes fruits, evidence, or an instrumentality of a crime. *Cf. Klitzman, Klitzman & Gallagher v. Krut*, 744 F.2d 955, 960 (3d Cir. 1984) (holding that the argument a warrant authorizing search of law firm records was overbroad carried “substantial support” because it allowed law enforcement agents to search *open* personal injury files when the probable cause showing established only that *closed* or *inactive* files were probative of an alleged mail fraud conspiracy). Indeed, it is not clear how probable cause could exist to search services that the government does not even know about, or that it cannot identify. At the very least, the warrant should identify those services, and the magistrate should be made aware of the vast scope of information sought. Instead, the warrant requests data from “any” Google service used by the subject accounts, indicating that the government has not established probable cause for each such service.

Because the warrant is unconstitutionally overbroad, Google should not be compelled to produce any further records until the government identifies the specific Google services for which it has established probable cause to search.

C. The NDO Is an Unconstitutional Prior Restraint on Speech

The NDO prohibits Google from “disclos[ing] in any manner, directly or indirectly, by any action or inaction, the existence of this order or search warrant, or this investigation, or Order of the Court, to the listed subscriber/user or to any other person, in full or redacted form, unless and until otherwise authorized to do so by the Court,” except to an attorney for purposes

of obtaining legal advice. *See* Order, at 1.⁴ The SCA does not authorize a court to impose an indefinite nondisclosure obligation and even if it did, such an obligation would be an unconstitutional “prior restraint” on speech. At minimum, the NDO must be amended to include a fixed period of nondisclosure and to allow appropriately redacted public filings regarding litigation over the enforcement of the warrant.

The SCA permits a court to order a provider not to disclose the existence of an order or warrant for a finite period which the court deems appropriate. *See* 18 U.S.C. § 2705(b). The statutory text requiring that any non-disclosure obligation imposed by the court upon a provider be “for [a] period . . . the court deems appropriate” would be mere surplusage—meaningless text—if the court were permitted to impose an indefinite non-disclosure obligation. Congress is presumed to have said what it meant and to have meant what it said, not to waste words or invite confusion, in drafting statutory text, and courts are required to interpret such text accordingly. *Connecticut Nat. Bank v. Germain*, 503 U.S. 249, 253-54 (1992) (“[C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says there.”); *Official Committee of Unsecured Creditors of Cybergene Corp. ex re. Cybergene Corp. v. Chinery*, 330 F.3d 548, 556 (3rd Cir. 2003) (same). Here, that means a non-disclosure order must be limited by an appropriate period.

Not surprisingly, therefore, multiple opinions addressing governmental requests to indefinitely prohibit service providers from disclosing legal process compelling the production of electronic records have rejected such requests and required that a court specify a definite period. For example, when the U.S. District Court for the Northern District of California confronted a

⁴ The NDO allows Google to disclose “the attached subpoena,” rather than the search warrant, to counsel. Google presumes this is a scrivener’s error that arose when the government incompletely revised its model proposed order to fit this application, suggesting that government seeks to impose an indefinite nondisclosure order on service providers whenever it obtains a search warrant for electronic records.

governmental request for an indefinite gag order essentially identical to the NDO at issue here, it held that the SCA's statutory nondisclosure authorization allowed only "[a] limited period of nondisclosure, as justified by the government's initial application." *In Matter of Search Warrant for [Redacted]@hotmail.com (Hotmail)*, 74 F. Supp. 3d 1184, 1186 (N.D. Cal. 2014). The court reasoned that a specific end date was required by the plain terms of 18 U.S.C. § 2705(b) and in consideration of "the First Amendment rights of both [the service provider] and the public, to say nothing of the rights of the target." *Id.* Accordingly, the court denied the government's request for an indefinite nondisclosure order, but allowed it "to submit a renewed request justifying a finite period." *Id.*; *see also In re Grand Jury Subpoena for: [Redacted]@yahoo.com*, 79 F Supp. 3d 1091, 1091 (N.D. Cal. 2015) (holding that an order prohibiting Yahoo from disclosing the existence of a grand jury subpoena for an indefinite period "would amount to an undue prior restraint of Yahoo!'s First Amendment right to inform the public of its role in searching and seizing its information"); *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders (Pen Trap)*, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008) (holding that "a fixed expiration date on sealing and non-disclosure of electronic surveillance orders is not merely better practice, but required by law; in particular, the First Amendment prohibition against prior restraint of speech and the common law right of access to judicial records").

The NDO at issue here raises the same constitutional concerns and warrants the same result because it indefinitely prohibits Google from disclosing the search warrant to the affected users or to the public. A judicial order that forbids certain communications before they occur, like the NDO, is a paradigmatic prior restraint on speech. *See Alexander v. United States*, 509 U.S. 544 (1993). There is a "heavy presumption" against the constitutional validity of such prior restraints. *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963); *see also NAACP v. Button*,

371 U.S. 415, 438 (1963) (“Broad prophylactic rules in the area of free expression are suspect.”). To overcome this presumption, the government must demonstrate that the NDO satisfies strict scrutiny, which it cannot do here. *See Brown v. Entm’t Merchs. Ass’n*, 131 S. Ct. 2729, 2738 (2011).

First, it is far from clear that the NDO serves a compelling interest or that any particular harm would be likely to result from disclosure. One well-established purpose of the Fourth Amendment’s warrant requirement is to “notify[] the subject of the search that his privacy must yield to the public’s need for law enforcement.” *Christine*, 687 F.2d at 756. Notice of governmental surveillance, search, and seizure is also required to allow the public to evaluate whether the government is reasonably implementing its powerful investigative tools. *See United States v. Donovan*, 429 U.S. 413, 439 (1977) (“[P]ostintercept notice was designed . . . to assure the community that the wiretap technique is reasonably employed.”). The public may or may not approve of the government’s methods, “but it is difficult for them to accept what they are prohibited from observing.” *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 572, 575 (1980) (noting that the First Amendment requires “freedom of communication on matters relating to the functioning of government” absent an overriding interest). That surveillance, search, and seizure without notice is more achievable through electronic searches than through physical searches does not diminish these protections—indeed, it heightens their importance. *See, e.g., Riley v. California*, 134 S. Ct. 2473, 2494-95 (2014) (observing that cell phone technology, which allows private information to be carried in a person’s pocket, “does not make the information any less worthy of the protection for which the Founders fought”); *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (noting that “[t]he potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous” and “is

compounded by the nature of digital storage”); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (noting that the Fourth Amendment particularity requirement is “much more important” in the context of computer searches, because computers “increase[] law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs”).

In light of these underlying principles supporting a notice requirement, the SCA authorizes a court to issue a nondisclosure order only “if it determines that there is reason to believe that notification of the warrant . . . will result in” one of five consequences, including “flight from prosecution,” “destruction of or tampering with evidence,” “intimidation of potential witnesses,” or “otherwise seriously jeopardizing an investigation or unduly delaying a trial.” 18 U.S.C. § 2705(b)(2)-(5). The NDO recites these factors, finding that “there is reason to believe that notification of the existence of the search warrant will seriously jeopardize the investigation, including by giving targets an opportunity to flee, to destroy or tamper with evidence, to intimidate witnesses, and to change patterns of behavior.” NDO at 1 (citing 18 U.S.C. § 2705). But there is no indication, at least in the portion of the record available to Google, of which of these governmental interests disclosure would place in jeopardy, of any facts supporting this conclusion, or that the Court reached this conclusion after undertaking the requisite independent inquiry.

Second, even assuming the record adequately supports *some* need to limit disclosure, the NDO is not narrowly tailored to protect that interest. *See Frisby v. Schultz*, 487 U.S. 474, 485 (1988) (holding that a prohibition “is narrowly tailored if it targets and eliminates no more than the exact source of the ‘evil’ it seeks to remedy”). The NDO’s indefinite term means its temporal scope is not tailored *at all*. *See Hotmail*, 74 F.Supp.3d at 1186; *Pen Trap*, 562 F. Supp. 2d at 877-78 (S.D. Tex. 2008).

Google therefore requests that the NDO be amended to include a fixed period or date certain after which it will expire; if necessary, the government may obtain an extension by establishing that any risks justifying the present order still exist.

IV. CONCLUSION

For the reasons given above, Google requests that this Court deny the government's motion to compel and amend the NDO to include a fixed expiration date.

DATED: November 28, 2016

PERKINS COIE LLP

By:

William DeStefano
Stevens and Lee
1818 Market Street, 29th Floor
Philadelphia, PA 19103
Phone: 215.751.1941

Todd M. Hinnen (*pro hac vice* pending)
John R. Tyler (*pro hac vice* pending)

PERKINS COIE LLP
1201 Third Avenue, Suite 4900
Seattle, Washington 98101
Phone: 206.359.8000

Attorneys for Google Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In re Search Warrant No. 16-960-M-1	:	Misc. No. 16-960-M-01
to Google	:	
	:	<u>FILED UNDER SEAL</u>

DECLARATION OF JOHN R. TYLER IN SUPPORT OF GOOGLE INC.'S RESPONSE
TO ORDER TO SHOW CAUSE

I, JOHN R. TYLER, declare and certify as follows:

1. I am an attorney with the law firm of Perkins Coie LLP in Seattle, and am one of the attorneys representing non-party Google Inc. in the above-entitled action. I have personal knowledge of the facts set forth in this declaration and am competent to testify.

2. Attached as Exhibit A is a true and correct copy of the cover letter Google sent on August 18, 2016, accompanying a production to the government of the following information responsive to the search warrant issued in this case: basic subscriber information, contacts, search history, browsing history, Android and Gmail content, to the extent such Gmail content was determined to be stored in the United States. This production excluded Gmail messages with attachments, because they were not confirmed to have been stored in the United States, and the production letter stated that Google's production was made consistent with the Second Circuit's decision in *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. (Microsoft)*, 829 F.3d 197 (2d Cir. 2016).

3. On November 10, 2016, I contacted Assistant United States Attorney James Petkun via email to inform him that Google intend to produce additional information to the government. To provide the government with additional time to review the supplemental production, I asked whether the government was amenable to a short continuance of Google's deadline for responding to the motion. On November 11, 2016, AUSA Petkun agreed via email

to a short continuance, which the parties submitted to the court on November 14, 2016. Attached as Exhibit B is a true and correct copy of my email thread with AUSA Petkun.

4. Attached as Exhibit C is a true and correct copy of the cover letter Google sent on November 11, 2016, accompanying a production to the government of the following additional information responsive to the warrant: header information associated with the emails that had attachments, as well as the content of those email messages, but not the attachments themselves (which were not confirmed to be stored in the United States).

5. On November 16, 2016, I spoke by telephone with AUSA Petkun regarding Google's production. During this call, I confirmed that contrary to the government's suggestion in its motion to compel that Google withheld Gmail content from prior to October 2013, Google had not withheld any content on that basis. I further confirmed that Google had produced all responsive Gmail content that Google confirmed was stored in the United States.

6. On November 23, 2016, I accessed the Google Help Center, available at <https://support.google.com/?hl=en>, which lists over a hundred Google services. Attached as Exhibit D is a true and correct copy of this page.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed on November 28, 2016.

By: */s/ John R. Tyler*
John R. Tyler